Invensys Operations Management Document "993754-1-905, Revision 3, Project Management Plan" (Non-Proprietary)

invensys™
Operations Management

Project:	PG&E PROCESS PROTECTION SYSTEM REPLACEMENT
Purchase Order No.:	3500897372
Project Sales Order:	993754

PACIFIC GAS & ELECTRIC COMPANY

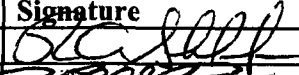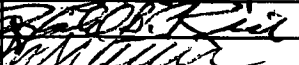## NUCLEAR SAFETY-RELATED PROCESS PROTECTION SYSTEM REPLACEMENT DIABLO CANYON POWER PLANT
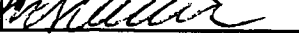
PROJECT MANAGEMENT PLAN (PMP)

Document No. 993754-1-905 (-NP)

Revision 3

December 18, 2012

	Name	Signature	Title
Author:	Roman Shaffer		Project Manager
Approvals:	Harry Rice		Project QA Manager
	Mark Herschthal		Director, Nuclear Delivery

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	2 of 82	Date:	12/18/2012	

Document Change History				
Revision	**Date**	**Change**	**Author**	
0	7/29/2011	Initial Issue for Use.	R. Shaffer	
1	10/13/2011	Revised to discuss control of Project Instructions, and incorporate Invensys Operations Management organizational changes.	R. Shaffer	
2	03/02/2012	Revised for Project Phase 2 updates throughout, including: • Additional document deliverables negotiated with PG&E for Project Phase 2 (and revised Appendix A); • The use of Subcontractor(s) during Project Phase 2 (Figure 4); • Updated discussion of Constraints and Assumptions in Section 3.3; • Updated discussion of risk management in Section 3.4;and • Updated discussion of work packages in Section 5.1 based on revised Invensys scope for Project Phase 2 negotiated with PG&E.	R. Shaffer	
		Revised Table 1 description of DTTA protective function.		
		Updated references to Invensys Corporate Nuclear Quality Assurance Manual.		
		Minor editorial changes throughout.		
		Editorial changes throughout for clarity, including: • Updates to address the full project (i.e., Phases 1 and 2); • Corrected references to documents in the References Section; and • Update the list of acronyms.		
		Revised the following Sections to reference the implementing sections of the PPM: 1.4, 2.2, 2.3, 2.4, 3.2, 3.3.2, 3.6.1.		
		Section 2.2 – Revised document listing based on scope negotiated with PG&E for both Nuclear Delivery and Nuclear IV&V; minor editorial changes to address both project phases.		
		Sections 2.4 and 5.3 – Revised to account for additions to Nuclear IV&V staff.		
3	12/18/2012	Editorial and formatting changes throughout.	R. Shaffer	
		Updated "Invensys Proprietary Information" footer.		
		Section 1.1 – Updated Figure 1 and descriptive text to add second Maintenance Workstation computer for the ALS; updated Interlock C-5 in Table 1.		
		Section 2.2 – Updated PPS Replacement Project organization chart in Figure 3.		
		Section 2.4 – Updated project assignments		
		Section 3.5.4 – Corrected reference to PPM 7.02.		

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	3 of 82	Date:	12/18/2012	

Table of Contents

invensys
™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	4 of 82	Date:	12/18/2012

List of Tables

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	6 of 82	Date:	12/18/2012	

List of Figures

i n v e n s y s
TM
Operations Management

i n v e n s y s
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	7 of 82	Date:	12/18/2012

1. Introduction

1.1. Project Overview

The Pacific Gas & Electric (PG&E) Diablo Canyon Power Plant (DCPP) Process Protection System (PPS) Replacement Project upgrades the existing Westinghouse Eagle 21 safety system. The scope of the equipment replacement is shown in the red box in Figure 1, below. The red box represents the Process Protection racks that contain the safety-related equipment.

The PPS monitors plant parameters, compares them against setpoints and provides signals to the Solid State Protection System (SSPS) if setpoints are exceeded. The SSPS evaluates the signals and performs Reactor Trip System (RTS) and Engineered Safety Feature Actuation System (ESFAS) functions to mitigate the event that is in progress. The SSPS, RTS, and ESFAS functions are not within the scope of the PPS Replacement Project.

PWR Protection Concept
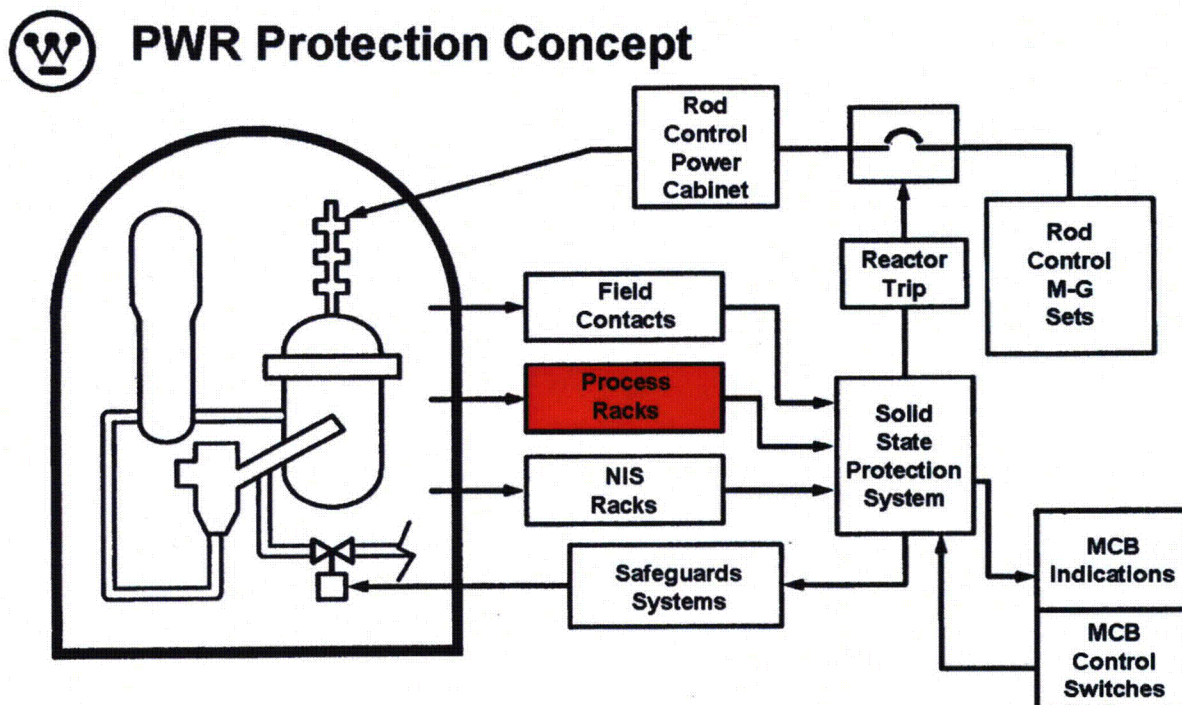
Figure 1. Westinghouse PWR Reactor Protection Concept [Ref. 1.5.1.2]

The PPS comprises four Protection Sets in sixteen racks. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	8 of 82	Date:	12/18/2012

penetrations, and process Protection Sets to the two redundant trains in the SSPS logic racks. Redundant process channels are separated by locating the electronics in different Protection Sets.

As shown in Figure 2, the replacement Protection Sets (I thru IV) each comprise the V10 Tricon, the Westinghouse Advanced Logic System (ALS) platform, the Maintenance Workstations, and various interface devices, such as the NetOptics Network Aggregator Tap and instrument loop isolators. The ALS and its associated Maintenance Workstation computer is not within Invensys Operations Management scope of supply. However, the ALS converts sensor inputs to a signal type compatible with the V10 Tricon hardware. Specifically, the ALS processes resistance temperature detector (RTD) inputs and converts them to 4-20 milliamp signals. This conversion is necessary to satisfy Diablo Canyon Power Plant loop accuracy requirements. See the Functional Requirements Specification [Ref. 1.5.1.3] for additional information.

The V10 Tricon portion of the PPS Replacement System comprises three V10 Tricon chassis per Protection Set: one safety-related Main Chassis, one safety-related Remote Expansion Chassis (RXM), and one nonsafety-related RXM chassis – see Figure 2. The Network Aggregator Tap, which is intended as an isolation device between the Tricon and the nonsafety plant network, is provided by PG&E to Invensys Operations Management for factory acceptance testing. The media converter, between the Tricon Main Chassis and the Network Aggregator Tap, will be provided by Invensys Operations Management and is necessary to convert the fiberoptic medium at the output of the Tricon Communication Module (TCM) to copper medium at the input of the Network Aggregator Tap.

The Maintenance Workstation is a nonsafety device developed separately from the PPS Replacement Project under a separate PG&E Purchase Order, budget, and staff. Development of the Maintenance Workstation is handled under a different project plan and by a separate project team. However, the Maintenance Workstation is part of the factory acceptance test of the V10 Tricon Protection Sets, as discussed in the Validation Test Plan, 993754-1-813. The technical requirements for the Tricon-to-Maintenance Workstation interface are provided in PG&E Interface Requirements Specification [Ref. 1.5.1.4].

The functions required in each V10 Tricon Protection Set are listed in Table 1 below. See the Functional Requirements Specification for additional details on the protection functions and their design bases. As can be seen in Table 1, the PPS Protection Sets do not have the same channel safety functions. This difference among Protection Sets influences the PPS Replacement Project approach to hardware and software development, and independent verification and validation. The Conceptual Design Document [Ref 1.5.1.2] and Functional Requirements Specification have additional detail on the hardware configuration of the PPS.

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	9 of 82	Date:	12/18/2012

Figure 2. Tricon Protection Set Architecture for the PPS Replacement System

The four Protection Sets have different hardware and software requirements. The Main Chassis in each Protection Set executes the TriStation 1131 application code (the PT2 file), therefore the PPS requires four application programs (four PT2 files). The application programs are developed as nuclear safety-related Software Integrity Level 4 (SIL4) software [Ref. 1.5.3.1]. Because of the differences between the Protection Sets, four sets of design documents are developed for the nuclear safety-related software. One of the following is developed for each Protection Set:

invensys

TM

Operations Management

invensys

Triconex

Table 1. V10 Tricon PPS Protection Set Channel Safety Functions

Channel(s) Function	Purpose	Protection Set			
		I	II	III	IV
Wide Range Reactor Coolant Temperature Channels					
Input to Low Temperature Overpressure Protection System (LTOPS)	Provides protection against over-pressurization at low plant temperature	X	X		
Wide Range Reactor Coolant Pressure Channels					
Input to LTOPS	Provides protection against over-pressurization at low plant temperature			X	X
Input to Residual Heat Removal (RHR) valve interlock circuit	Provides protection against improper operation of RHR isolation valves			X	X
Delta-T / Tavg (DTTA) Channels					
Overtemperature Delta-T (OTDT) Reactor Trip	Provides DNB protection	X	X	X	X
Overpower Delta-T (OPDT) Reactor Trip	Provides protection against excessive power (fuel rod rating protection)	X	X	X	X
Low-Low T_{avg} P-12	Blocks steam dump to prevent undesired cooldown	X	X	X	X
Low T_{avg} Feedwater Isolation	Prevents excessive cooling after trip to maintain shutdown margin	X	X	X	X
Pressurizer Level Channels					
Pressurizer High Water Level Reactor Trip	• Provides backup protection to the Pressurizer High Pressure Reactor Trip, and • Prevents the pressurizer from becoming water solid during low-worth and -power rod withdrawal accidents	X	X	X	
Pressurizer Vapor Temperature Channel					
Pressurizer Vapor Space Temperature Low	RHR valve V-8701 interlock circuit input				X
Steam Generator Steam Flow Channel					
Steam Flow Indication	Provide safety-related outputs for post-accident monitoring (S/G 1 thru 4)	X	X		
Steamline Break Protection Channels					
Steamline Pressure Low SI and Steamline Isolation	• Initiate the automatic starting of boron injection and decay heat removal systems and • Provide protection against steamline break accidents	X	X	X	X
Steamline Pressure High Negative Rate Steamline Isolation	Provide protection in the case of a steamline break when Pressurizer Pressure is less than the P-11 setpoint and Low Steamline Pressure SI is blocked	X	X	X	X
Steam Generator Narrow Range Level Channels					
Steam Generator (S/G) High-High Level Turbine Trip and Feedwater Isolation (P-14, S/G High Level Permissive)	Provides protection against S/G overfill and damage to the main steamlines or main turbine	X	X	X	X
S/G Low-Low Level Reactor Trip and Auxiliary Feedwater (AFW) Pump Start	Protects the reactor from loss of heat sink in the event of loss of feedwater to one or more S/Gs or a major feedwater line rupture	X	X	X	X
Turbine Impulse Chamber Pressure Channels					
Turbine Impulse Chamber Pressure High to P-13 Interlock	• Provide an input to P-7 indicative of low turbine power when less than the setpoint • P-7 permissive disables selected Reactor Trip signals at low power levels	X	X		

Document:	993754-1-905	Title:	Project Management Plan					
Revision:	3	Page:	11 of 82	Date:		12/18/2012		

Channel(s)	Purpose	Protection Set			
Function		I	II	III	IV
Turbine Impulse Chamber Pressure Low Interlock C-5	• Blocks control rod withdrawal • The purpose of the C-5 interlock is to prevent automatic outward rod motion when power is less than the design limit for the Rod Control System	X			

- Hardware Requirements Specification
- Software Requirements Specification
- Software Design Description
- Application Program (PT2 file)

The list of documents generated during the PPS Replacement Project is in Appendix A, with the project document numbering scheme provided in Appendix B. Additional discussion of project deliverables for PG&E is provided in Section 1.2.

A single Project Traceability Matrix, 993754-1-804, is maintained, but is formatted to facilitate requirements traceability for each Protection Set. Invensys document 993754-1-906, Software Development Plan, provides details on the application program development process. Invensys document 993754-1-910, Software Integration Plan, discusses the strategy for integrating the software and hardware for each Protection Set. Invensys document 993754-1-802, Software Verification and Validation Plan, discusses the strategy for performing independent verification and validation of the PPS application software. See Section 3.6 of this plan for details on staffing requirements for the PPS Replacement Project.

The SIL4 application code (i.e., PT2 file) that is executed on the safety-related Tricon Main Chassis is developed as safety-related software using approved processes and procedures that adhere to current regulatory requirements. Specifically, the Invensys Nuclear System Integration Program Manual (NSIPM) [Ref. 1.5.4.1] describes the overarching approach used during the PPS Replacement Project, as explained in the remaining sections of this Plan. The Project Procedures Manual (PPM) [Ref. 1.5.4.4] contains the implementing procedures. The independent verification and validation activities meet the intent of Institute of Electrical and Electronics Engineers (IEEE) Standard 1012 [Ref .1.5.3.1] for SIL 4 software.

Software and firmware related to the V10 Tricon platform and TriStation 1131 Developer Workbench are included in the U.S. NRC safety evaluation of the V10 Tricon Topical Report [Ref. 1.5.4.3]. The PPS Replacement Project activities do not develop or modify software or firmware related to either the V10 Tricon platform or TriStation 1131.

1.2. Project Deliverables

PG&E will submit a License Amendment Request (LAR) in accordance with Interim Staff Guidance-6 (DI&C-ISG-06) [Ref. 1.5.2.7]. The guidance contained in DI&C-ISG-06 specifies certain design documents that should be provided to the NRC to support the staff's review of a

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	12 of 82	Date:	12/18/2012

LAR application. Based on DI&C-ISG-06, the PPS LAR review is a Tier 2 review. The list of documents required by the staff for a Tier 2 review includes normal digital system design documentation, e.g., SRS, SDD, test plans, and so on, but also several other documents particular to the NRC regulatory review process.

The DI&C-ISG-06 Tier 2 review is divided into three phases:

    Phase 1 – Initial Application
    Phase 2 – Continued Review and Audit
    Phase 3 – System Implementation and Inspection

Enclosure B of DI&C-ISG-06 lists which documents should be submitted and/or available for audit during each of the above phases. To summarize, Phase 1 requires system software design documentation through the Software Requirements Specification as well as System Test Plan(s). Phase 2 requires software code listings as well as test documentation (e.g., test specifications and test reports). Phase 3, the system site-installation phase, requires Licensee project plans, user manuals, and test reports to be available for audit.

PG&E prefers that the PPS Replacement Project be funded in phases that are synchronized to the DI&C-ISG-06 Tier 2 review phases. PG&E Purchase Order 3500897372 [Ref. 1.5.1.1] identifies project document deliverables[1] for Project Phases 1 and 2. Invensys Operations Management PPS Replacement Project activities are managed with this Plan for the entire project scope (Phases 1 and 2). Section 2.1 describes the lifecycle applied during this project, including the mapping to DI&C-ISG-06 phased deliverables.

Appendix A lists the set of documents that Invensys Operations Management intends to deliver to PG&E for the PPS Replacement Project, separated into Phase 1 and Phase 2 deliverables. Section 2.1 describes the lifecycle applied during this project, including the mapping to DI&C-ISG-06 phased deliverables. The sequence follows the lifecycle applied by Invensys Operations Management – see Section 2.1 for further discussion. Appendix B shows the Invensys Operations Management document numbering scheme for the PPS Replacement Project.

The PPS V10 Tricon hardware will be ordered during Project Phase 2 after receiving written permission from PG&E. Ordering hardware prior to approved and released drawings requires a Conditional Release, in accordance with the NSIPM and PPMs. The risk is acceptable because the Hardware Requirements Specification for each Protection Set will have been released to PG&E for review and comment. Final assembly and release of the V10 Tricon Protection Set equipment for test does not proceed until system drawings are approved for use.

---

[1] At the time the Purchase Order was issued that DI&C-ISG-06 was still in draft form. Since then, Revision 1 of DI&C-ISG-06 has been released, and Appendix A reflects the changes since the Purchase Order was issued.

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	13 of 82	Date:	12/18/2012

PG&E is responsible for negotiating the DCPP LAR review schedule with the NRC. The detailed schedule, 993754-1-059, developed by Invensys Operations Management is synchronized with the LAR submittal dates provided by PG&E. As the LAR schedule changes, PG&E provides the updates to Invensys Operations Management and the detailed project schedule is updated accordingly.

All DI&C-ISG-06 LAR deliverables in Appendix A are scheduled for delivery to PG&E as shown in the PPS Replacement Project Schedule, 993754-1-059. The document deliverables are released to PG&E at various times for review and comment as shown in the detailed project schedule – see Section 5.5 for discussion of the PPS Replacement Project schedule.

1.3. Purpose of the Project Management Plan

This Project Management Plan (PMP) has been written to ensure that the management of the PPS Replacement Project conforms to NRC guidance for development of software intended for use in nuclear safety-related applications. This Plan was written to conform to Branch Technical Position 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems [Ref. 1.5.2.2], and NUREG/CR-6101 [Ref. 1.5.2.4].

This Plan describes the management process for the PPS Replacement Project to ensure adherence to the Invensys Operations Management quality and process requirements for the development of nuclear safety-related software and hardware. This Plan addresses the following areas:

- Project Organization – The Plan describes the organizational structure of the Invensys Operations Management project team, including organizational boundaries and interfaces to PG&E, PG&E subcontractors, and the NRC.
- Management Oversight - The Plan describes the management methods and tools used to oversee the work performed by the Invensys Operations Management project team.
- Organizational and Personnel Responsibilities - The Plan describes the duties of the Invensys Operations Management organizations involved in developing the PPS Protection Sets based on the V10 Tricon hardware and software, and of the individuals within each organization.
- Project Risks - The Plan describes the methods and tools used to identify, assess, and manage project risks that may interfere with achieving project objectives.
- Development Environment and Product Security - The Plan describes the methods used to protect project data and equipment from inadvertent or malicious alteration.

1.4. Evolution of the Project Management Plan

This Plan is controlled as a Configuration Item in accordance with the Invensys Operations Management Nuclear System Integration Program Manual (NSIPM), Section 10.0, as implemented by the Project Procedures Manual (PPM), Section 4.0, Project Document and Data

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	14 of 82	Date:	12/18/2012

Control. In accordance with the NSIPM, the PMP is listed on a master configuration list that identifies the current revision level of the PMP to ensure project personnel are using the approved version. The initial and subsequent releases of the PMP is reviewed and approved by the Project Manager and the Quality Assurance Manager prior to use by project personnel. Upon each release of the PMP for project use, the project Master Configuration List, 993754-1-803, is updated.

Release of any version of the PMP to PG&E is done in accordance with the NSIPM, Section 10, as implemented by PPM 4.0. See Invensys document 993754-1-909, Software Configuration Management Plan, for additional details on the Configuration Management activities during the PPS Replacement Project.

1.5. Reference Materials

1.5.1. PG&E Documents

1.5.1.1 PG&E Purchase Order 3500897372.

1.5.1.2 PG&E Process Protection System Replacement Conceptual Design Document.

1.5.1.3 PG&E Functional Requirements Specification, 08-0015-SP-001.

1.5.1.4 PG&E Process Protection System Replacement Interface Requirements Specification.

1.5.2. NRC Documents

1.5.2.1 NUREG-0800, Standard Review Plan, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition, Chapter 7 – Instrumentation and Controls, U.S. Nuclear Regulatory Commission.

1.5.2.2 Branch Technical Position 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, U.S. Nuclear Regulatory Commission.

1.5.2.3 Regulatory Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, U.S. Nuclear Regulatory Commission.

1.5.2.4 NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems, U.S. Nuclear Regulatory Commission.

1.5.2.5 DI&C-ISG-01, Digital Instrumentation and Controls Task Working Group #1: Cyber Security Interim Staff Guidance, U.S. Nuclear Regulatory Commission.

1.5.2.6 DI&C-ISG-04, Digital Instrumentation and Controls Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues Interim Staff Guidance, U.S. Nuclear Regulatory Commission.

1.5.2.7 DI&C-ISG-06, Digital Instrumentation and Controls Task Working Group #6: Licensing Process Interim Staff Guidance, U.S. Nuclear Regulatory Commission.

1.5.2.8 Title 10 of the Code of Federal Regulations, Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

1.5.2.9 Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, U.S. Nuclear Regulatory Commission.

1.5.3. Industry Documents

1.5.3.1 IEEE Standard 1012-1998, IEEE Standard for Software Verification and Validation.

1.5.3.2 NQA-1-1994, Quality Assurance Requirements for Nuclear Facility Applications.

1.5.3.3-IEEE Standard 1074-1995, IEEE Standard for Developing Software Life Cycle Processes.

1.5.4. Invensys Operations Management Documents

1.5.4.1 NSIPM, Nuclear Systems Integration Program Manual, NTX-SER-09-21.

1.5.4.2 QM-2, Invensys Operations Management Nuclear Quality Assurance Manual.

1.5.4.3 V10 Tricon Topical Report, 7286-1-545, Invensys Operations Management (ADAMS Accession Number ML110140443).

1.5.4.4 Project Procedures Manual, Invensys Operations Management.

1.5.4.5 Manufacturing Department Manual, Invensys Operations Management.

1.5.4.6 NTX-SER-10-14, V10 Tricon Conformance to Regulatory Guide 1.152.

1.5.4.7 Project Instruction 1.0, Application Project Administrative Controls for the PPS Replacement Project.

1.5.4.8 Project Instruction 7.0, Application Program Development for the PPS Replacement Project.

1.6. Definitions and Acronyms

1.6.1. Definitions

activity: A defined body of work to be performed, including its required Input and Output Information.

Configuration Item: A specification or product that is to be incorporated into the configuration management process.

constraint: A restriction on software life cycle process (SLCP) development.

integrity level: A denotation of a range of values of a property of an item necessary to maintain system risks within acceptable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.

invensys
TM
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	16 of 82	Date:	12/18/2012	

product: Any output of the software development Activities (e.g., document, code, or model).

Software Integrity Level (SIL): The integrity level of a software item.

software life cycle (SLC): The project-specific sequence of Activities.

work package: A work package is a subset of a project that can be assigned to a responsible individual or organization to complete a collection of work actions necessary to create a specific result; the lowest level of the work breakdown structure where both the cost and the duration can be reliably estimated.

1.6.2. Acronyms

AFW	Auxiliary Feedwater
ALS	Advanced Logic System
ANSI	American National Standards Institute
ASAI	Application Specific Action Item
ASME	American Society of Mechanical Engineers
CASE	Computer-Assisted Software Engineering
CDD	Conceptual Design Document
CFR	Code of Federal Regulations
DCPP	Diablo Canyon Power Plant
DI&C	Digital Instrumentation and Controls
EMI	Electromagnetic Interference
ESFAS	Engineered Safety Feature Actuation System
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FRS	Functional Requirements Specification
HRS	Hardware Requirements Specification
HSI	Human-System Interface
HVT	Hardware Validation Test
I/O	Input/Output
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOM	Invensys Operations Management
IRS	Interface Requirements Specification
ISG	Interim Staff Guidance
IV&V	Independent Verification and Validation
LAR	License Amendment Request
LLR	Lessons Learned Report
LOE	Level of Effort
LTOPS	Low Temperature Overpressure Protection System
MCB	Main Control Board
MCL	Master Configuration List

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	17 of 82	Date:	12/18/2012

MDM	Manufacturing Department Manual
ND	Nuclear Project Delivery
NQA	Nuclear Quality Assurance
NRC	U.S. Nuclear Regulatory Commission
NSIPM	Nuclear System Integration Program Manual
OPDT	Over-Power Delta-T
OTDT	Over-Temperature Delta-T
PAN	Product Alert Notice
PE	Project Engineer
PG&E	Pacific Gas & Electric Company
PMP	Project Management Plan
PO	Purchase Order
POCM	Purchase Order Compliance Matrix
PPM	Project Procedures Manual
PQAE	Project Quality Assurance Engineer
PQAM	Project Quality Assurance Manager
PQP	Project Quality Plan
PPS	Process Protection System
PRC	Project Review Committee
PT2	File extension for the TriStation 1131 application code, i.e., *.PT2
PTM	Project Traceability Matrix
PWR	Pressurized Water Reactor
QA	Quality Assurance
QC	Quality Controls
QPM	Quality Procedures Manual
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RHR	Residual Heat Removal
RTS	Reactor Trip System
RXM	Remote Extender Module, Remote Expansion Chassis
S/G	Steam Generator
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SDD	Software Design Description
SDP	Software Development Plan
SER	Safety Evaluation Report
SI	Safety Injection
SIL	Software Integrity Level
SIntP	Software Integration Plan
SLC	Software Life Cycle
SLCP	Software Life Cycle Process
SQAP	Software Quality Assurance Plan

invensys

TM

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	18 of 82	Date:	12/18/2012	

SRS	Software Requirements Specification
SSP	Software Safety Plan
SSPS	Solid State Protection System
SVVP	Software Verification and Validation Plan
SWR	Software Walkthrough Report
TAB	Technical Advisory Bulletin
TAN	Technical Application Note
TCM	Tricon Communications Module
TRL	Technical Requirements List
TS1131	TriStation 1131
TSAP	TriStation Application Project
V&V	Verification and Validation

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	19 of 82	Date:	12/18/2012

2.   Project Organization

2.1. Process Model

Invensys Operations Management project scope is limited to design of the V10 Tricon portion of the PPS hardware and software and Factory Acceptance Testing. As an approved 10 CFR Part 50 Appendix B supplier, Invensys Operations Management adheres to the Invensys Nuclear Systems Integration Program Manual (NSIPM) to ensure compliance with NRC requirements regarding safety-related software development. The Invensys Operations Management Quality Procedures Manual (QPM), Project Procedures Manual (PPM), and Manufacturing Department Manual (MDM) are the implementing procedures under the NSIPM.

The Invensys Operations Management PPM requires a project lifecycle comprising several phases. The overlap between the DI&C-ISG-06 LAR review phases and the NSIPM project lifecycle phases is shown in Table 4, below. Section 1.2 of this plan provides more detail on the DI&C-ISG-06 Enclosure B documents that are produced during PPS Replacement Project Phases 1 and 2.

Table 2. Lifecycle Mapping

PPS Project	DI&C-ISG-06 Enclosure B	NSIPM Project Lifecycle Phase
Phase 1	Phase 1	Acquisition
		Planning
		Requirements
		Design (until completion of software design description and test plans)
Phase 2	Phase 2	Design (remainder of Enclosure B documents)
		Implementation
		Test
		Delivery
█████████	Phase 3	Scope of Supply **To Be Determined**

Discussion of the detailed project schedule is provided in Section 5.5.

2.2. Organizational Structure

The organizational structure for the Invensys Operations Management project team is shown in Figure 3. The figure shows the organizations involved in the PPS Replacement Project, which includes Nuclear Delivery (ND), Nuclear Quality Assurance (NQA), and Nuclear Independent Verification and Validation (IV&V). The following is a description of the role of each organization, assigned project responsibilities, and document deliverables. A summary of the responsibilities of each position shown in Figure 3 are provided in Section 2.4. Additional details are provided in the NSIPM with supplemental details in the PPM.

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	20 of 82	Date:	12/18/2012

ND is responsible for project execution, system hardware and software design, software implementation, system construction, and system delivery (during project Delivery Phase). PPS Replacement Project Team members from ND include the PM, PE, Hardware Design team, Software Design team, and support staff as needed (a project Administrative Assistant, test engineers, etc.). Ultimately, ND is responsible for the quality and safety of the delivered PPS, and for delivering the V10 Tricon Protection Sets within budget and schedule constraints. ND is responsible for producing the following documents:

P

Nuclear IV&V is responsible for ensuring that ND has adequately met the safety system requirements as defined in contract documents, Design Input documents, regulatory requirements, and Invensys Operations Management procedures. As shown in Figure 3, Nuclear IV&V is independent of ND to ensure Nuclear IV&V is not be adversely impacted by schedule pressure and financial/budget constraints. PPS Replacement Project Team members from Nuclear IV&V include the IV&V Team Lead and three IV&V Engineers. Nuclear IV&V is responsible for the following:

P

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	21 of 82	Date:	12/18/2012

P

NQA is responsible for ensuring that ND and Nuclear IV&V are adhering to applicable procedures and processes for nuclear safety-related system development, such as the Invensys Operations Management QM-2 corporate Nuclear Quality Assurance Manual [Ref. 1.5.4.2], the QPM and PPM. As shown in Figure 3, NQA is also sufficiently independent of ND to ensure the reporting chain is not unduly influenced by ND. NQA is responsible for the following:

1) Project Quality Plan, 993754-1-900
2) Software Quality Assurance Plan, 993754-1-801
3) Audits and surveillances during the project

ND interfaces with Nuclear IV&V staff and NQA as needed. When anomalies have been identified during the project lifecycle, cases may arise that require escalating the resolution to higher levels of Management within Invensys Operations Management. In Figure 3, the lines of communication between the organizations at the Management and Director levels are shown by the dashed lines. As shown, issues requiring escalation can be escalated up separate and independent reporting chains up to the Director level. In those rare cases that the Director level is not sufficient, QM-2 allows escalation to the Regional and Global Director levels and still

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	22 of 82	Date:	12/18/2012

maintain the necessary managerial, technical, and financial independence necessary for compliance to NRC requirements contained in, for example, Regulatory Guide 1.168 [Ref. 1.5.2.3].

This Project Plan is revised appropriately if the PPS Replacement Project organizational structure depicted in Figure 3 changes. This may entail changes to Figure 3, addition of project personnel, changes to project responsibilities, or changes in the reporting structure.
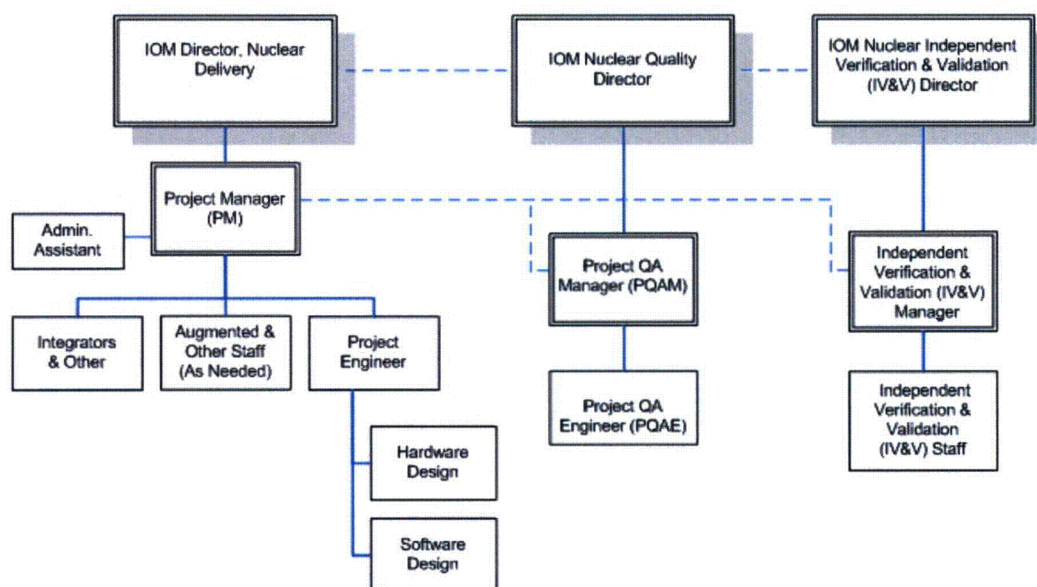
Figure 3. PPS Replacement Project Organizational Structure

It is important to note that if any change in the organizational structure depicted in Figure 3 impact the organizational independence between Nuclear IV&V and Nuclear Delivery, project activity must stop and an assessment made as to the impact on regulatory commitments related to the V10 Tricon Safety Evaluation. The assessment determines if project mitigation measures are necessary to ensure compliance with NRC requirements regarding independence of the Nuclear IV&V staff. Any mitigation measure(s) could require that this Project Plan be revised appropriately (and in accordance with the NSIPM, Section 10.0, as implemented by PPM 4.0). The assessment, conclusions, and any necessary mitigation measures are documented and handled in accordance with the NSIPM as implemented in the PPM.

2.3. Organizational Boundaries and Interfaces

PG&E is the customer and nuclear licensee pursuing the License Amendment Request (LAR) for Diablo Canyon Power Plant (DCPP). As such, PG&E is the project/system integrator responsible for overall project execution, and creation and submittal of the LAR package. PG&E has contracted with both Westinghouse and Invensys Operations Management for the PPS

invensys
TM
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	23 of 82	Date:	12/18/2012

Replacement Project. All interactions between Westinghouse and Invensys Operations Management pertinent to the PPS Replacement Project are at the direction of and coordinated by PG&E.

PG&E also utilizes the engineering services of Altran Solutions (Altran). Both PG&E and Altran could provide technical input and direction to Invensys Operations Management. Any technical direction provided by Altran must first be approved by the PG&E Project Manager.

The single point of contact within Invensys Operations Management for external interactions is the Project Manager or designee. Certain technical questions and coordination of project meetings may be handled by the Project Engineer after first discussing it with the Project Manager. For issues related to Nuclear IV&V and NQA, the Project Manager or designee coordinates the interactions with PG&E and/or Altran.

All interactions with the NRC are coordinated by and through PG&E. Figure 4 shows the organizational boundaries among the various entities.

Invensys Operations Management will subcontract engineering services from Technology Resources for the reliability analysis of the V10 Tricon PPS Replacement during Project Phase 2. Technology Resources is currently assisting Invensys-Foxboro with the reliability analysis for a large-scale nuclear project for an international customer. Based on previous experience with Technology Resources personnel, Technology Resources has the technical expertise and regulatory experience to perform the work on the PPS Replacement.

The Project Manager is responsible for the technical interface with Technology Resources (and other subcontractors, if needed) to ensure day-to-day tasks are on track with schedule and technical expectations. The subcontractor services are procured in accordance with the NSIPM, Section 11.0, as implemented by PPM 5.0, and any design outputs from the subcontractor reviewed, managed, and controlled in accordance with NSIPM Sections 4.0, 7.0, 8.0, 9.0, and 10.0 (as implemented by PPMs 2.0, 4.0, 9.0, and 10.0).

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	24 of 82	Date:	12/18/2012
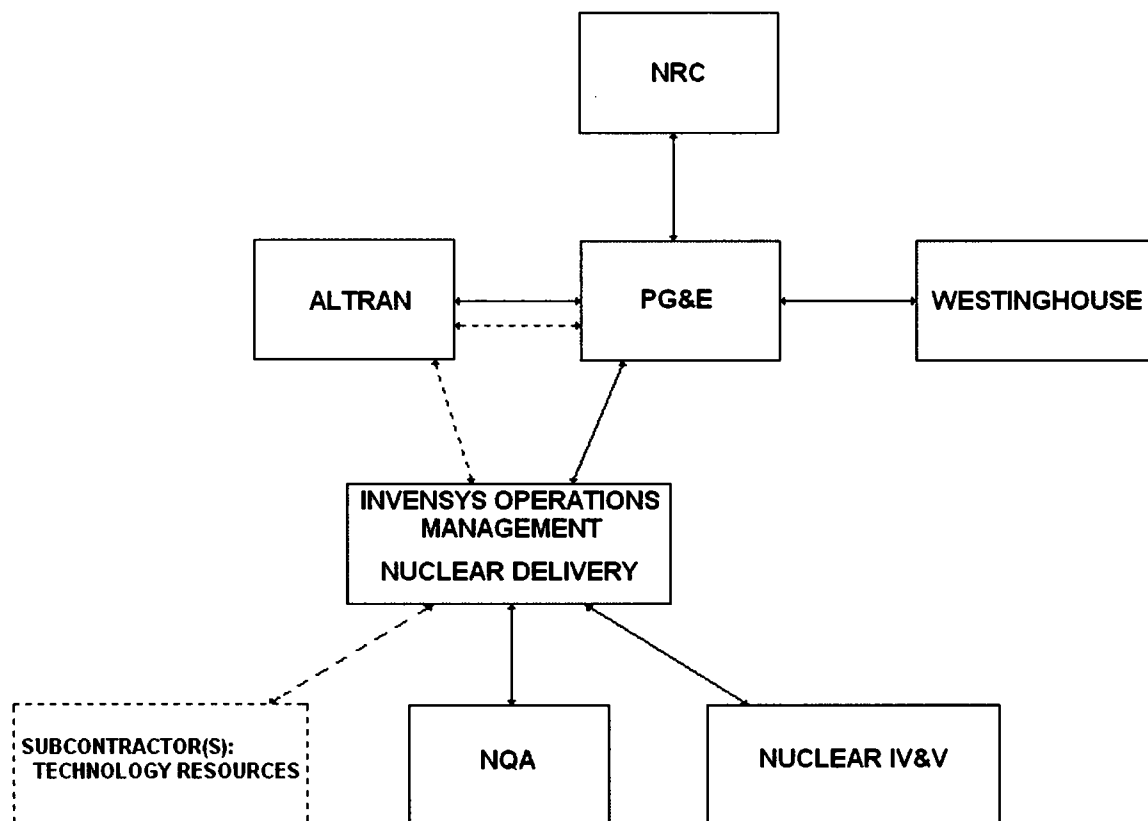
Figure 4. PPS Replacement Project – Interface Boundaries

2.4. Project Responsibilities

Invensys Operations Management has assigned a core group of engineers and support staff to the PPS Replacement Project. As project needs change, assigned personnel are added or removed. The following individuals are involved in the PPS Replacement Project:

P

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	25 of 82	Date:	12/18/2012	

P

invensys™

Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	26 of 82	Date:	12/18/2012	

P

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	28 of 82	Date:	12/18/2012	

P

Changes to the organization chart or position responsibilities could require a revision to this Project Plan. If necessary, the Project Plan is revised in accordance with the NSIPM, Section 10.0, as implemented by PPM 4.0.

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	29 of 82	Date:	12/18/2012	

3. Managerial Process

3.1. Management Objectives

The primary management objective is to produce the safety-related V10 Tricon Protection Sets within the authorized budget limitations negotiated with PG&E by the scheduled submittal date for the Diablo Canyon Power Plant License Amendment Request. Progress against schedule and hours expended per work package (see Section 5) is tracked and measured against the risk factors identified in Section 3.4. Negative trends with regard to schedule and hours expended is assessed for appropriate compensatory measures, including:

1) Identifying work-process efficiencies,
2) Adding project personnel, and
3) Increasing the "Not to Exceed" value of Project Phase 1 (requires PG&E approval).

Section 3.4 discusses project risk management.

Adherence to the NSIPM and the implementing procedures in the PPM, QPM, and MDM is essential to achieving project quality objectives in accordance with the Invensys Operations Management Appendix B program. The project schedule and negotiated budget (schedule and cost) were developed based on the life cycle defined in the NSIPM as implemented by the PPM. Adhering to the procedures also assures the required project deliverables satisfy PG&E technical and NRC regulatory requirements, and that the necessary supporting collateral is generated to support the safety conclusions of both ND and Nuclear IV&V. Quality metrics are identified in the Software Quality Assurance Plan, 993754-1-801.

3.2. Management Priorities

P

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	30 of 82	Date:	12/18/2012	

Issues related to anomalies, non-conformances, and process deficiencies will be addressed with the utmost care in accordance with the NSIPM, Sections 7.0 and 8.0 (as implemented by PPM 10.0).

3.3. Assumptions, Dependencies and Constraints

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	31 of 82	Date:	12/18/2012	

P

3.4. Risk Management

The major risk factors are summarized below. Section 3.4 discusses monitoring and control mechanisms to mitigate the identified risk factors.

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	32 of 82	Date:	12/18/2012	

P

invensys

I

P

3.5. Monitoring and Controlling Mechanisms

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	34 of 82	Date:	12/18/2012	

P

3.5.4. Project Phase Summary Reports and Exit Meetings

In accordance with the Invensys Operations Management process, the Phase Exit Meetings occur at the end of the current project life cycle phase (e.g., Requirements, Design, Implementation, Test) and is a prerequisite to entering the subsequent phase.

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	35 of 82	Date:	12/18/2012

P

3.5.5. Project Review Committee

The Project Review Committee is composed of the Project Manager, Project Engineer, Project Quality Assurance Engineer, and Nuclear IV&V/Test Director. The Project Review Committee will meet for PPS Project phase related activities as follows:
- Phase Exit Meetings – The Project Review Committee reviews project activities associated with the current phase, evaluates the risks, and provides recommendations associated with lessons learned prior to transitioning to the subsequent phase.
- Other – The Project Review Committee reviews and evaluates additional project activities as deemed appropriate by the Project Manager.

3.5.6. NQA Audits and Surveillances

Invensys document 993754-1-900, Project Quality Plan, describes the overarching project quality requirements contained in the PG&E Purchase Order [Ref. 1.5.1.1] and purchase specification documents [References 1.5.1.2, 1.5.1.3, and 1.5.1.4]. The project Software Quality Assurance Plan, 993754-1-801, describes the NQA activities to ensure the project quality requirements and Invensys methods and procedures are being followed. This includes the various audits and surveillances conducted during the PPS Replacement Project.

3.6. Staffing Plan

Technical expertise for the PPS Replacement Project Team is found from a combination of available Invensys Operations Management staff and external staff augmentation resources. During Project Phase 2 the reliability analysis of the V10 Tricon portion of the PPS Replacement will be performed by a subcontractor on the nuclear approved suppliers list.

3.6.1. Skill levels required

The PPS Replacement Project requires a ND project team with combined knowledge and experience with the U.S. NRC regulations and processes, software engineering lifecycle management, and technical design and implementation of nuclear safety-related hardware and software. Specific skills and knowledge are required in the following areas:
1) Design and procedural compliance with 10 CFR Part 50, including Appendices A and B
2) Application of U.S. NRC Regulatory Guides relevant to safety-system software development
3) Application of relevant U.S. NRC staff guidance related to design of nuclear safety systems, such as Branch Technical Position 7-14 [Ref. 1.5.2.2] and DI&C-ISG-01 [Ref. 1.5. 2.5], DI&C-ISG -04 [Ref. 1.5.2.6], and DI&C-ISG -06 [Ref. 1.5.2.7]

I

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	36 of 82	Date:	12/18/2012

4) Understanding of staff guidance contained in Chapter 7 of U.S. NRC NUREG-0800, Standard Review Plan [Ref. 1.5.2.1]

5) Application of relevant Institute of Electrical and Electronics Engineers standards (e.g., those endorsed by U.S. NRC Regulatory Guides) to nuclear safety-related system design and implementation

6) Implementation of the Invensys Operations Management NSIPM and PPM to nuclear safety-related projects

7) Nuclear safety and protection systems

8) Tricon system hardware design and construction

9) Tricon application code (PT2 file) development using TriStation 1131

In *addition to* the above skill sets for the ND project team, the Nuclear IV&V team requires specific skills and knowledge in the following areas:

1) Application of U.S. NRC Regulatory Guides relevant to independent verification and validation safety-system software

2) Application of Institute of Electrical and Electronics Engineers standards (e.g., those endorsed by U.S. NRC Regulatory Guides) relevant to independent verification and validation of software for nuclear safety-related applications

In *addition to* the above skill sets for the Nuclear IV&V team, the NQA Project Quality Assurance Engineer requires specific skills and knowledge in the following areas:

1) Invensys Operations Management PPMs

2) Invensys Operations Management corporate Nuclear Quality Policy, QM-2 [Ref. 1.5.4.2]

3) U.S. NRC Appendix B criteria [Ref. 1.5.2.8] and application of such criteria to nuclear safety-related projects involving hardware and software design

4) NQA-1 criteria [Ref. 1.5.3.2] and application of such criteria to nuclear safety-related projects involving hardware and software design

See Section 2.0 for a detailed discussion of the PPS Replacement Project Organizational Structure (Section 2.2) and project team members' responsibilities (Section 2.4). Training files, including experience summaries, for the PPS Replacement Project team members are maintained by the Project Administrator. Changes to the project team could require an update to this plan, which will be done in accordance with NSIPM Section 10.0 as implemented by PPM 4.0.

3.6.2. Start times and duration of needs

A constant staffing level is used during PPS Replacement Project Phase 1. Project activities remain at a constant level up to the scheduled delivery dates for Phase 1 project deliverables. Staffing levels during Project Phase 2 will change based on project life cycle. During the Design Phase augmented staff will be utilized for some of the project activities, as well as third-party engineering services from Technology Resources. During Implementation Phase augmented staff will be utilized to assist with staging the V10 Tricon PPS Replacement equipment in

invensys
Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	37 of 82	Date:	12/18/2012

preparation for validation testing during the Test Phase. At the end of the Implementation Phase there will be a drop off in Nuclear Delivery resources as the project will enter into the Test Phase, which is predominantly Nuclear IV&V scope. Nuclear Delivery personnel will remain active to support the project as needed, but the expectation is a maximum of half-time level of effort. Section 5.3 discusses resource requirements in more detail.

3.6.3. Training requirements

Project personnel shall be appropriately qualified and trained in accordance with the NSIPM Section 9.0 and PPM 9.0, Personnel Training and Qualification. A copy of project personnel qualification and training records is included in the PPS Replacement Project document file.

P

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	38 of 82	Date:	12/18/2012

P

Specialized Training. The Project Quality Assurance Engineer requires specialized training, because of the project responsibilities performed by the Nuclear Quality Assurance organization. Specifically, personnel performing inspection activities shall be qualified and certified in accordance with Invensys Operations Management QPM 18.2. Other specialized training will be assigned as needed on a case-by-case basis.

Training records for the PPS Replacement Project Team are handled in accordance with the NSIPM as implemented by the PPM and QPM with regard to Quality Records and retention.

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	39 of 82	Date:	12/18/2012	

4. Technical Process

4.1. Methods, Tools and Techniques

The PPS Replacement Project team adheres to the NSIPM and utilizes the PPM as the implementing set of procedures. The PPM defines a modified Waterfall model, as shown in Figure 5, based upon NQA-1 [Ref. 1.5.3.2]. The guidance contained in NQA-1-1994 was utilized in preparing the PPM to ensure compliance with all nuclear quality requirements. The PPM is a combination of different procedures, including forms specified for use in the various PPM procedures. The PPM is a controlled document, and each procedure within the PPM is revision-controlled with its own revision level. Forms, which are to be used during project implementation, are also revision-controlled documents. The PPM contains a compliance matrix showing compliance with 10 CFR Part 50 Appendix B [Ref. 1.5.2.8] and NQA-1-1994.

4.1.1. Computing systems to be used for software development

Equipment and tools used by the Invensys Operations Management project team during the project lifecycle are listed below. Control of material (e.g., test equipment, safety-related V10 Tricon hardware, and so on) and equipment calibration (e.g., for hardware validation and factory acceptance testing) is handled in accordance with the NSIPM as implemented by the PPM.

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	40 of 82	Date:	12/18/2012

P

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	41 of 82	Date:	12/18/2012
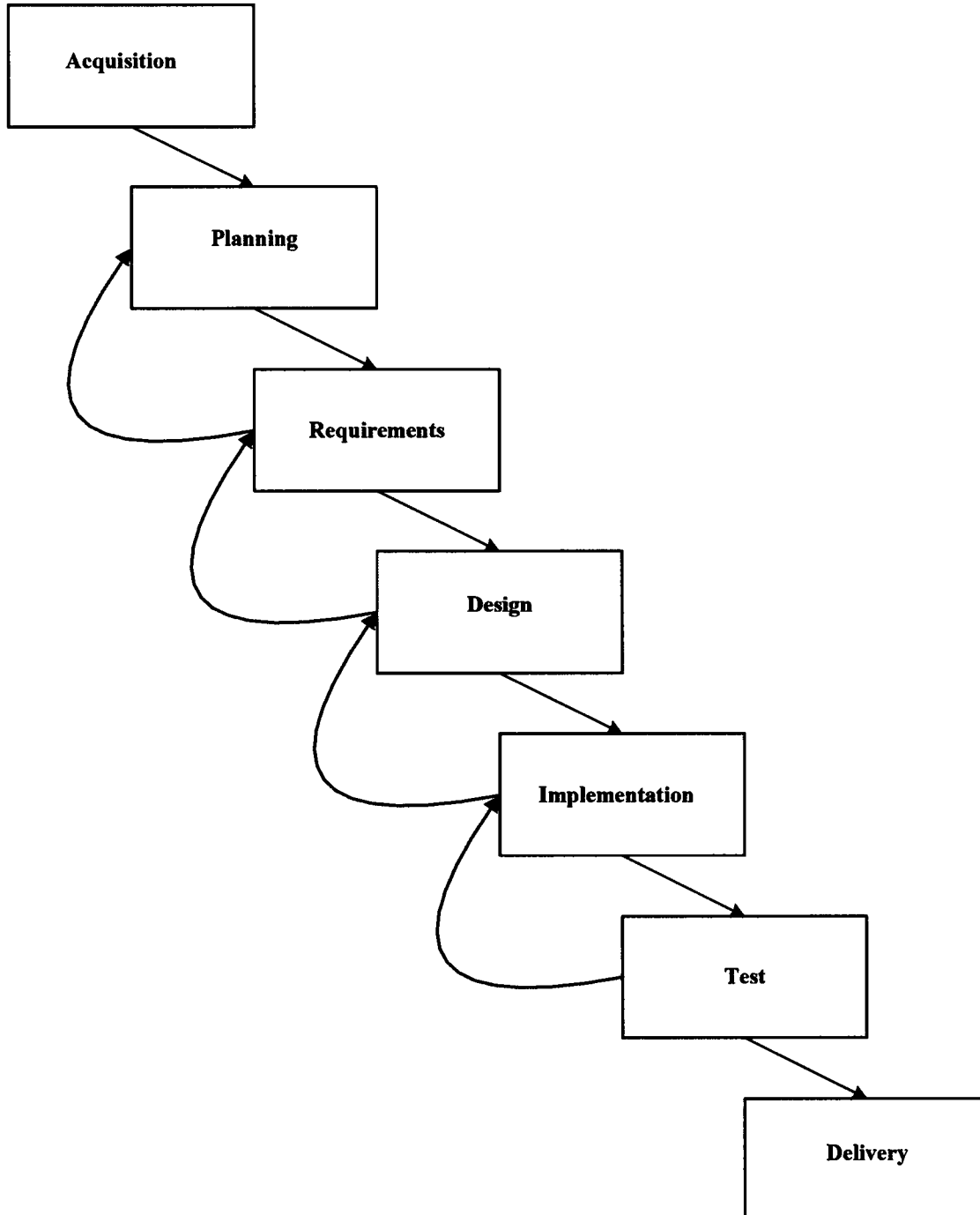
Figure 5. Invensys Nuclear Integration Project Waterfall Lifecycle

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	42 of 82	Date:	12/18/2012

4.1.2. Development methods

The NSIPM as implemented by the PPM follows a modified Waterfall software development methodology in conformance to IEEE Std 1074 [Ref. 1.5.3.3]. Project management controls are utilized in each lifecycle phase to ensure phase activities are performed in accordance with the NSIPM as implemented by the PPM. Additional details of the technical process are found in the PPS Replacement Project Software Development Plan, 993754-1-906.

4.1.3. Programming languages

TriStation 1131 provides three programming languages that comply with the IEC 61131-3 standard: Function Block Diagram, Ladder Diagram, and Structured Text. An optional language, CEMPLE (Cause and Effect Matrix), has not been qualified by Invensys Operations Management for use in developing software intended for nuclear safety-related applications.

For the PPS Replacement Project, the following programming languages are utilized when developing the V10 Tricon Protection Set application code:
* Function blocks
* Structured Text

Section 4.1.7 discusses the programming guidelines described in 993754-1-907, PPS Replacement Project Coding Guidelines.

4.1.4. Computer-assisted software engineering (CASE) tools

None.

4.1.5. Technical standards to be followed

Replacement of the Diablo Canyon Power Plant Process Protection System requires NRC approval prior to installation of the V10 Tricon Protection Sets. PG&E intends to submit the License Amendment Request package to the NRC for review. There are a number of regulatory requirements that must be satisfied, such as 10 CFR 50.55a(h), which incorporates IEEE Standard 603-1991 by reference, the General Design Criteria contained in Appendix A, and Appendix B quality and design criteria,as well as a number of regulatory guidance documents. The regulatory guidance documents endorse consensus standards from the Institute of Electronics and Electrical Engineers (IEEE). The following standards and guidance are used as developmental references for all PPS Replacement Project documents.

It should be noted that the V10 Tricon platform safety evaluation assessed Invensys Operations Management against these same requirements and guidance. Therefore, the below list is focused on the PPS application development aspects, rather than on the entire set of documents expected for a Tier 2 review as defined in NRC DI&C-ISG-06.

invensys™

invensys

Operations Management

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	43 of 82	Date:	12/18/2012	

NRC Staff Review Guidance:
* NUREG-0800, Standard Review Plan, Chapter 7
* Branch Technical Position 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

Regulatory Guides:
* 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
* 1.168, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
* 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
* 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
* 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
* 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
* 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-related Instrumentation and Control Systems
* 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

Nuclear Regulatory Reports:
* NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems

IEEE standards:
* 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
* 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
* 730, IEEE Standard for Quality Assurance Plans
* 828, IEEE Standard for Configuration Management Plans
* 829, IEEE Standard for Software Test Documentation
* 830, IEEE Recommended Practice for Software Requirements Specifications
* 1012, IEEE Standard for Software Verification and Validation
* 1016, IEEE Recommended Practice for Software Design Descriptions
* 1028, IEEE Standard for Software Reviews and Audits
* 1058, IEEE Standard for Software Project Management Plans
* 1059, IEEE Guide for Software Verification and Validation Plans
* 1074, IEEE Standard for Developing Software Life Cycle Processes
* 1228, IEEE Standard for Software Safety Plans

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	44 of 82	Date:	12/18/2012

Other standards:
- ANSI/ASME NQA-1-1983, Quality Assurance Program Requirements for Nuclear Facilities
- ANSI/ASME NQA-1a-1983 (Addenda), Addenda to ANSI/ASME NQA-1-1983, Quality Assurance Program Requirements for Nuclear Facilities
- ANSI/ASME NQA-1-1994, the basis for the PPM

4.1.6. Company development procedures

As an approved 10 CFR Part 50 Appendix B supplier, Invensys Operations Management adheres to the Invensys Nuclear Systems Integration Program Manual (NSIPM) to ensure compliance with NRC requirements regarding safety-related software development. The Invensys Operations Management Quality Procedures Manual (QPM), Project Procedures Manual (PPM), and Manufacturing Department Manual (MDM) [Ref. 1.5.4.5] are the implementing procedures under the NSIPM. These procedures have been audited numerous times by third parties, including the NRC, and found compliant with a 10 CFR Part 50 Appendix B program as well as the NRC requirements for development of safety-related software.

QM-2: This is the corporate policy manual applicable to nuclear safety-related activities at Invensys Operations Management facilities. The corporate Nuclear Quality Assurance Manual, QM-2, governs the quality affecting activities performed by ND personnel at Invensys Operations Management facilities. Nuclear quality affecting activities are conducted in accordance with the QM-2 and the Project Quality Plan, 993754-1-900.

NTX-SER-09-21: This is the Nuclear System Integration Program Manual. This program manual is the overarching lifecycle document for nuclear system integration projects, and it is currently being reviewed by the NRC as part of the V10 Tricon safety evaluation.

Project Procedures Manual: This manual contains the ND implementing procedures under the NSIPM. The PPM describes the process lifecycle for nuclear safety system integration projects.

Quality Procedures Manual: Defines the quality (implementing) procedures for nuclear safety-related activities. This program manual is not specific to integration projects, but rather for any issue pertinent to nuclear safety-related activities, materials, and systems. NQA is predominantly responsible for the implementation of the QPM procedures.

Manufacturing Department Manual: This manual defines the manufacture, assembly, and test activities for Tricon components. It describes assembly and test of nuclear safety-related Tricon systems, including the tools for and controls over the manufacturing of printed circuit boards, modules, power supplies, and chassis, among other things. It also addresses receiving and shipment of materials.

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	45 of 82	Date:	12/18/2012	

4.1.7. Company programming style

Coding Guidelines, 993754-1-907, contains guidance for the ND staff regarding TriStation 1131 project configuration, application code layout, tagname convention, and general guidance on programming style. The guidance also discusses proper usage of the PPS-specific function blocks in the V10 Tricon Protection Set application code. Product and technical advisories and bulletins (i.e., PANs, TAN, and TAB) relevant to the V10 Tricon are listed along with necessary compensating actions.

P

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	46 of 82	Date:	12/18/2012	

4.2. Software Documentation

Appendix A contains a sequential list of documents that Invensys Operations Management produces for PG&E during the PPS Replacement. The sequence follows the lifecycle applied by Invensys Operations Management as discussed in Section 2.1.

The Software Development Plan, 993754-1-906, provides a detailed discussion of the technical documents required for the development of the V10 Tricon Protection Set application code

The PPS Replacement Project Software Verification and Validation Plan, 993754-1-802, provides additional details on the verification and validation activities performed by Nuclear IV&V and the documents generated during verification and validation activities. The Software Quality Assurance Plan, 993754-1-801, defines the quality affecting activities to be followed in the design, development, review, and testing for the PPS Replacement Project to ensure the specified quality requirements are met.

4.3. Project Support Functions

Project support functions are those functions that are not performed by ND, but are essential to ensure the quality of the V10 Tricon Protection Sets meet PG&E requirements. The below functions are inherent in the Invensys Operations Management Nuclear System Integration process and procedures.

4.3.1. Software Quality Assurance

Software Quality Assurance is performed by the Nuclear Quality Assurance organization. Project responsibilities are defined in the Software Quality Assurance Plan, 993754-1-801.

4.3.2. Software Configuration Management

Software configuration management is the responsibility of ND. Nuclear IV&V verifies adequate configuration control and document the analysis in the project phase reports. Project responsibilities are defined in the Software Configuration Management Plan, 993754-1-909.

4.3.3. Software Verification and Validation (including testing)

Software Verification and Validation is the responsibility of Nuclear IV&V. Project responsibilities are defined in the Software Verification and Validation Plan, 993754-1-802.

4.3.4. Software Safety Management

Software Safety Management is the responsibility of Nuclear IV&V. Project responsibilities are defined in the Software Safety Plan, 993754-1-911.

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	47 of 82	Date:	12/18/2012	

4.3.5. Software reviews and audits

Software reviews are the responsibility of ND and NQA. The Software Development Plan, 993754-1-906, describes the software reviews performed by ND. Reviews and audits performed by NQA are defined in the Software Quality Assurance Plan, 993754-1-801, and the Invensys Operations Management QPM.

4.3.6. User Software Documentation

User software documentation for the V10 Tricon Protection Sets is not within the scope of the PPS Replacement Project.

invensys™

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	48 of 82	Date:	12/18/2012	

5.   Work Packages, Schedule, and Budget

5.1. Work Packages

A work package is a subset of the PPS Replacement Project that can be assigned to a responsible individual/organization to complete a collection of work actions necessary for a specific result, such as: 1) develop a design output (e.g., document, application code); 2) review a design output (including documentation); or 3) complete a test (e.g., verification, validation). The work packages for the PPS Replacement Project are the lowest level of the work breakdown structure where both the cost and the duration can be reliably estimated.

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	49 of 82	Date:	12/18/2012

P

P

invensys
Operations Management

invensys
Triconex

invensys I

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	51 of 82	Date:	12/18/2012	

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	52 of 82	Date:	12/18/2012	

P

invensys

I

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	53 of 82	Date:	12/18/2012

P

invensys

invensys

I

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:		Project Management Plan		
Revision:	3	Page:	54 of 82	Date:	12/18/2012	

P

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	56 of 82	Date:	12/18/2012	

P

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	57 of 82	Date:	12/18/2012	

P

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	58 of 82	Date:	12/18/2012

P

invensys™

Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	59 of 82	Date:	12/18/2012

P

/

invensys™

Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	60 of 82	Date:	12/18/2012	

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	61 of 82	Date:	12/18/2012

P

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	63 of 82	Date:	12/18/2012

5.2. Dependencies

As stated in Section 4.1, The PPS Replacement Project team adheres to the NSIPM and utilize the PPM as the implementing set of procedures. The PPM defines a modified Waterfall model. At the macroscopic level, Figure 5 depicts the Waterfall lifecycle dependencies among the phases. These dependencies mean that Design Outputs from a subsequent project phase cannot be issued to Nuclear IV&V for independent review without first exiting the current phase. At the project implementation level, the various work packages related to planning and technical documents (Design Outputs) have dependencies within project phases. The significant dependencies are shown in Table 4.

P

The PPS Replacement Project Software Development Plan, 993754-1-906, contains more details on the dependencies and procedures for working with conditionally released Design Outputs.

5.3. Resource Requirements

The PPS comprises four Protection Sets (I thru IV), with each set composed of three V10 Tricon chassis. Because of the differences between the Protection Sets, four sets of documents are developed – one of the following for each Protection Set:
- Hardware Requirements Specification
- Software Requirement Specification
- Software Design Description
- Application Program (PT2 file)

P

I

P

I

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	65 of 82	Date:	12/18/2012	

P

invensys

Operations Management

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	66 of 82	Date:	12/18/2012

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	67 of 82	Date:	12/18/2012	

6. Additional Components

6.1. Project Security Requirements

Invensys Operations Management utilizes several layers of defense to ensure protection of sensitive customer information and equipment. Invensys document NTX-SER-10-14 [Ref. 1.5.4.6] describes the Invensys Operations Management security controls over personnel, physical, and network access to nuclear safety-related equipment and data. NTX-SER-10-14 describes the controls to ensure a secure development environment for the V10 Tricon platform to meet regulatory commitments to maintain conformance with Regulatory Guide 1.152. These same controls are utilized on the PPS Replacement Project supplemented with the following project specific requirements. Invensys document 993754-1-913, PPS Replacement Project: Conformance to RG1.152, provides the Regulatory Guide 1.152 compliance matrix for the PPS replacement project.

6.1.1. Physical Access Controls

Physical Security of the Development Environment. Access into the Invensys Operations Management facility requires a picture badge and keycard. Guests, including PG&E visitors, must check in at the front desk to obtain a guest badge and meet their sponsor from Invensys Operations Management.

Entry to the ND test floor where the V10 Tricon Protection Sets is staged is limited to ND and Nuclear IV&V personnel only. Guests, including PG&E, are escorted at all times while on the ND test floor.

P

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	68 of 82	Date:	12/18/2012

P

6.1.3. Project Controls and Application Security

P

invensys

I

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan		
Revision:	3	Page:	69 of 82	Date:	12/18/2012

P

V10 Tricon Protection Set Application Code. Role-Based access to the TriStation 1131 project file (PT2) for the V10 Tricon Protection Sets will be configured in accordance with the following:

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan			
Revision:	3	Page:	70 of 82	Date:	12/18/2012	

7. Appendices

Appendix A – PPS Replacement Project Documents List

Appendix B – PPS Replacement Project Document Numbering Scheme

Appendix B – PPS Replacement Project Hours Tracking Sheets

Appendix C – PPS Replacement Project Required Reading Lists

invensys™
Operations Management

invensys
Triconex

Appendix A – PPS Replacement Project Documents List

The table below lists the project documents generated for the PPS Replacement Project according to Project Phase. Not all documents are project deliverables to PG&E, indicated in the table below in the "Deliverable" column. The "PMP" and "SDP" columns indicate where the document is described, either the Project Management Plan, or the Software Development Plan, 993754-1-906. The descriptions of project documents generated by Nuclear IV&V are in the relevant planning document (e.g., SVVP, SSP).

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix A		
Revision:	3	Page:	72 of 82	Date:	12/18/2012

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix A		
Revision:	3	Page:	73 of 82	Date:	12/18/2012

P

invensys
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix A		
Revision:	3	Page:	74 of 82	Date:	12/18/2012

P

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix B		
Revision:	3	Page:	75 of 82	Date:	12/18/2012

Appendix B – PPS Project Document Numbering Scheme

The document numbering scheme in the below table is taken from PPMs 3.0 and 4.0, with most of the listed documents from the latter. Table 4.2, Project Document Number Scheme, has been modified for the PPS Replacement Project. The table below includes documents from NRC Branch Technical Position 7-14 and Interim Staff Guidance 6.

P

invensys™

Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix B	
Revision:	3	Page:	76 of 82	Date:	12/18/2012	

P

invensys™

Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix B			
Revision:	3	Page:	77 of 82	Date:	12/18/2012	

PPM 3.0 provides the standard Invensys Operations Management numbering scheme for project construction drawings (mechanical, electrical, function block diagrams, etc.).

invensys™
Operations Management

invensys
Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix C		
Revision:	3	Page:	78 of 82	Date:	12/18/2012

Appendix C – PPS Replacement Project Hours Tracking Sheets

invensys™

Operations Management

PROJECT MAN-HOURS TRACKING SHEET

PROJECT/SO#	PG&E DCPP Process Protection System Replacement Project/SO993754 (US0153311)
WEEK ENDING DATE	

NAME	TASK	% Complete	HOURS	COMMENTS

invensys

Operations Management

invensys

Triconex

Document:	993754-1-905	Title:	Project Management Plan – Appendix D		
Revision:	3	Page:	80 of 82	Date:	12/18/2012

Appendix D – PPS Replacement Project Required Reading Lists